PTO/SB/08a/b (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 4

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Abdulhakim Nobahar
Attorney Docket Number	44424162-8721

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	V54	US - 4,309,569	01-05-1982	Merkle	
	V55	US - 5,434,919	07-18-1995	Chaum	

U.S. PATENT DOCUMENTS PURSUANT TO McKESSON (notices of allowance)

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Notices of Allowance mailed:
	8712	US 20030028771 A1	02-06-2003	Paul C. Kocher et al.	12-07-2007
	8724	US 2001/0053220 A1	12-20-2001	Paul C. Kocher et al.	11-28-2007

U.S. PATENT DOCUMENTS PURSUANT TO McKESSON (related patents & applications)

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	U.S. Patent Application no. and date filed
	0097	US 2006/0045264 A1	03-02-2006	Paul C. Kocher et al.	11/252,898 03-02-2006
	0140	US 2008/0022146 A1	01-24-2008	Paul C. Kocher et al.	11/643,349 12-21-2006
	0167	USSN 11/977,392		Paul C. Kocher et al.	11/977,392 1/24/2007
	0168	USSN 11/981,495		Paul C. Kocher et al.	11/981,495 10/30/2007
	0169	USSN 11/978,364		Paul C. Kocher et al.	11/978,364 10/29/2007
	8710	US 6,304,658 B1	10-16-2001	Paul C. Kocher et al.	
	8711	US 6,381,699 B1	04-30-2002	Paul C. Kocher et al.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 4

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Abdulhakim Nobahar
Attorney Docket Number	44424162-8721

U.S. PATENT DOCUMENTS PURSUANT TO McKESSON (related patents & applications)

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	U.S. Patent Application no. and date filed
	8712	US 2003/0028771 A1	02-06-2003	Paul C. Kocher et al.	10/136,012 04-29-2002
	8718	US 6,298,442 B1	10-02-2001	Paul C. Kocher et al.	
	8720	US 6,327,661 B1	12-04-2001	Paul C. Kocher et al.	
	8723	US 6,278,783 B1	08-21-2001	Paul C. Kocher et al.	
	8724	US 2001/0053220 A1	12-20-2001	Paul C. Kocher et al.	09/930,,836 August 15, 2001
	8726	US 6,539,092 B1	03-25-2003	Paul C. Kocher et al.	
	8727	US 2003/0188158 A1	10-02-2003	Paul C. Kocher et al.	10/396,975 03-24-2003
	8730	US 6,510,518 B1	01-21-2003	Paul C. Kocher et al.	
	8731	US 6,654,884 B1	11-25-2006	Paul C. Kocher et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/08a (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 3 of 4

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Abdulhakim Nobahar
Attorney Docket No.	44424162-8721

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	CiteNo.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	V56	SCHNEIER, Bruce, Applied Cryptography, Chapter 12, pp. 265-301, John Wiley & Sons, Inc. (2d. Ed. 1996), New York, NY.	
	V57	Grounds Of Opposition, European Patent 1092297 in the name of Cryptography Research, Inc., Opposition by Visa Europe Services, Inc., January 25, 2008.	
	V58	Posting on sci.crypt newsgroup, KOCHER, Paul C et al., "Announce: Timing cryptanalysis of RSA, DH, DSS" et al., messages 1-51 of 51, Dec. 11, 1995 through Dec. 24, 1995, http://groups.google,com/group/sci.crypt	
	V59	DAEMEN, Joan, "Management of Secret Keys: Dynamic Key Handling", Course on Computer Security and Industrial Cryptography (COSIC '97 - June 1997) Presentation Slides; and declaration of Professor Bart Preneel dated 15 June 2007.	
	V60	DAVIES & PRICE, Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer, 2nd Ed., John Wiley & Sons, New York, NY, 1989, pp. 318-321.	
	V61	PIPER, F., Key Management (Part 3.5) ZERGO: Information Security Training Club, Hampshire, U.K., January 1993, Foils 6-18 to 6-30.	
	V62	PIPER, F., Declaration of, Jan. 21, 2008, University of London, England.	
	V63	BRADLEY, S., "Derived Unique Key Per Transaction Schemes," Some Applications of Mathematics to the Theory of Communications, Ch. 4, pp. 132-199, Ph.D. Thesis, University of London, England, 1994.	
	V64	ISO (International Organization for Standardization), Banking - Key management (retail) , "Part 3: Key life cycle for symmetric ciphers", ISO 11568-3 First edition, December 1, 1994, pp. 1-16, www.saiglobal.com/shop	
	V65	American National Standard for Financial Services, secretariat - American Bankers Association (ANS/ABA X9.24-200x), Key Management Using Triple DEA and PKI, revised by Terry Benson, American National Standards Institute, September 12, 2000.	
	V66	MENZES, A.J. et al., Handbook of Applied Cryptography, pp. 71, 586, 636-637, CRC Press, Boca Raton, Florida (1997).	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a/b (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	4	of	4

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Abdulhakim Nobahar
Attorney Docket No.	44424162-8721

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	CiteNo.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	V67	Interbank Card Association, PIN Manual: A Guide to the Use of Personal Identification Numbers in Interchange, pp. 61- 127, 1979.	
	V68	SEDGEWICK, Robert, Algorithims, 2nd Ed., Chs. 4 and 11, Addison-Wesley, Arlington, VA, 1988.	
	V69	BRASSARD, Gilles, "On computationally secure authentication tags requiring short secret shared keys", Adv. of Crypt.: Proceedings of Crypto-82, D. Chaum, R.L. Rivest, and A.T. Sherman, Eds. Plenum Press, New York, NY, 1982, pp. 79-86.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.